EBOOK

Sécuriser votre identité avec Proofpoint

Cas d'utilisation et témoignages de réussite

proofpoint.

Introduction

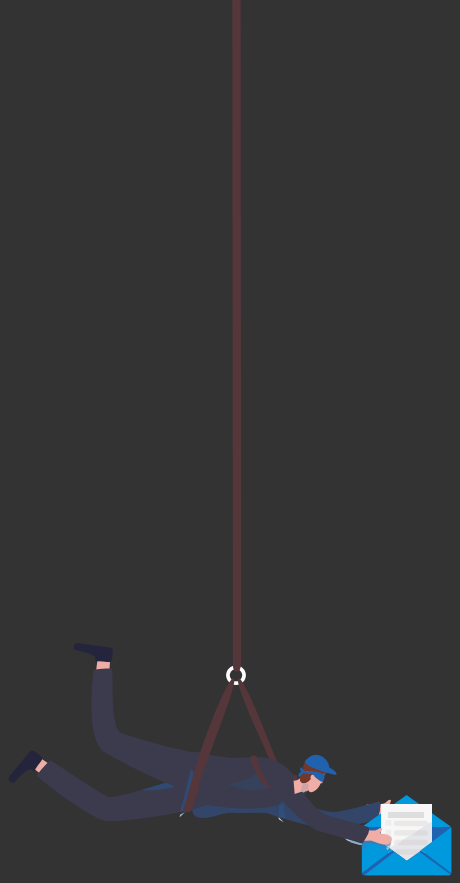
L'élévation des privilèges et le déplacement latéral constituent un défi constant pour la plupart des équipes de sécurité, même dans les plus grandes entreprises du monde. Microsoft en est le parfait exemple. En janvier 2024, l'entreprise a annoncé avoir été victime d'une compromission à l'instigation d'un célèbre groupe cybercriminel soutenu par la Russie.

Les cyberpirates ont exploité un ancien compte de test laissé sans protection. Une fois le compte compromis, ils ont élevé ses privilèges et se sont déplacés latéralement sur les systèmes cloud de Microsoft. Mais voilà le hic : comme ils se faisaient passer pour des utilisateurs légitimes, ils ont échappé à toute détection pendant plus d'un mois[1].

Les compromissions comme celles-ci mettent en lumière la faiblesse du milieu de la chaîne d'attaque. C'est là que les cybercriminels utilisent des comptes compromis pour percer les couches suivantes des défenses d'une entreprise. Pour ce faire, ils exploitent des erreurs de configuration et identifient des vulnérabilités liées aux identités pour obtenir un accès à des comptes disposant de privilèges de plus en plus élevés.

Élévation des privilèges et déplacement latéral

1 Bleeping Computer, « Microsoft Reveals How Hackers Breached Its Exchange Online Accounts » (Microsoft révèle comment des cyberpirates ont compromis ses comptes en ligne Exchange), janvier 2024.



Cette partie de la chaîne d'attaque joue un rôle déterminant dans les cyberattaques. Avec une identité volée, les cybercriminels ressemblent à s'y méprendre à des utilisateurs légitimes, ce qui les rend invisibles. Et puisqu'ils sont invisibles, ils peuvent faire pratiquement tout ce qu'ils veulent : réinitialiser des mots de passe, modifier des règles, installer des logiciels, extraire et chiffrer des données pour demander une rançon, etc.

Qu'est-il possible de faire pour les stopper ?

Proofpoint Identity Protection vous fournit les analyses dont vous avez besoin pour identifier vos identités vulnérables et les corriger avant que des cybercriminels ne mettent la main dessus. Mais pas seulement. Il permet également de mettre en lumière les cybercriminels actifs une fois qu'ils ont infiltré votre environnement.

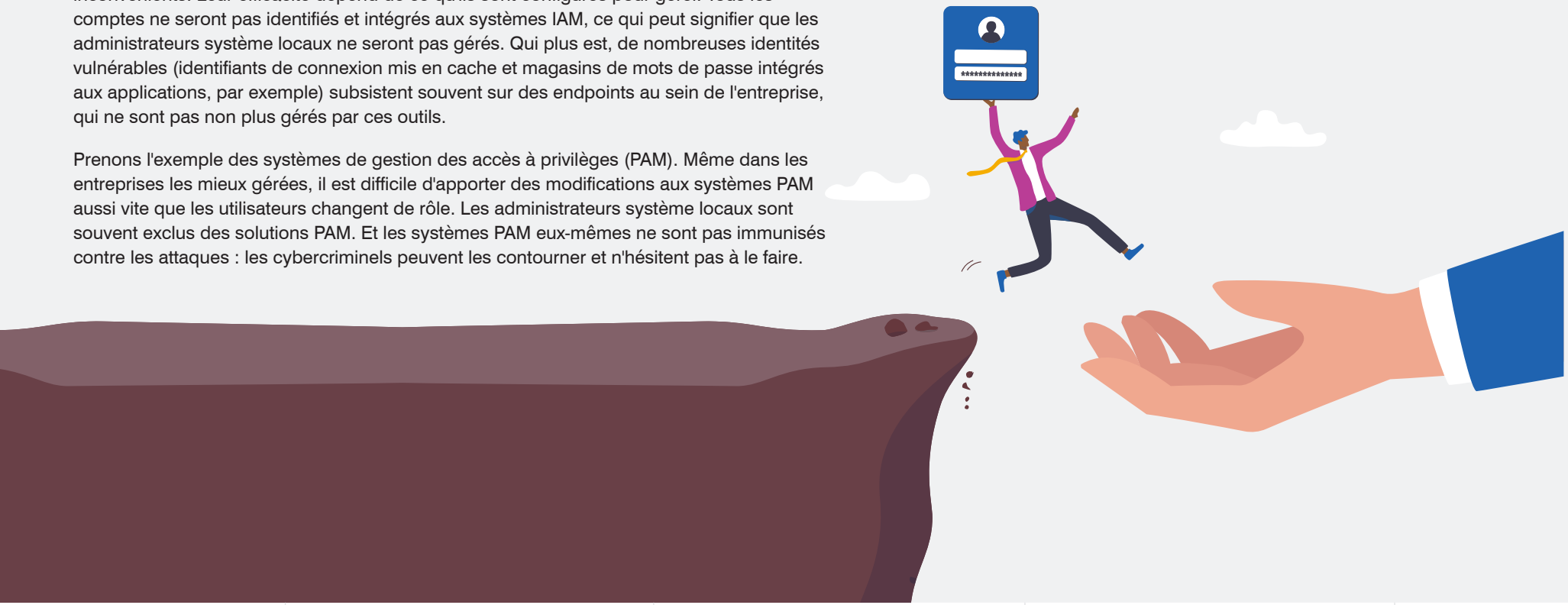
Cet eBook présente trois cas d'utilisation destinés à illustrer le fonctionnement de cette solution. Il contient également des témoignages clients afin de vous montrer à quoi Proofpoint Identity Protection ressemble en action.

CAS D'UTILISATION 1 :

Corriger les failles de sécurité laissées par les outils IAM

Tous les outils courants de gestion des identités et des accès (IAM) partagent les mêmes inconvénients. Leur efficacité dépend de ce qu'ils sont configurés pour gérer. Tous les comptes ne seront pas identifiés et intégrés aux systèmes IAM, ce qui peut signifier que les administrateurs système locaux ne seront pas gérés. Qui plus est, de nombreuses identités vulnérables (identifiants de connexion mis en cache et magasins de mots de passe intégrés aux applications, par exemple) subsistent souvent sur des endpoints au sein de l'entreprise, qui ne sont pas non plus gérés par ces outils.

Prenons l'exemple des systèmes de gestion des accès à privilèges (PAM). Même dans les entreprises les mieux gérées, il est difficile d'apporter des modifications aux systèmes PAM aussi vite que les utilisateurs changent de rôle. Les administrateurs système locaux sont souvent exclus des solutions PAM. Et les systèmes PAM eux-mêmes ne sont pas immunisés contre les attaques : les cybercriminels peuvent les contourner et n'hésitent pas à le faire.



Résumé

Une entreprise de financement automobile utilise Proofpoint pour étendre ses fonctionnalités de sécurité afin d'inclure la gestion des risques liés aux identités.

Profil client

Secteur d'activité : Finance

Collaborateurs : 9 000

Lieu : Monde

Solution

Produit : Proofpoint Identity Protection

Composant : Proofpoint Spotlight

Comment Proofpoint peut vous aider

Composant de Proofpoint Identity Protection, Proofpoint Spotlight vous aide à identifier vos identités vulnérables et à corriger les failles de sécurité de vos identités avant que les cyberpirates ne les exploitent. Pour ce faire, il analyse vos endpoints, les systèmes IAM et les référentiels d'identités afin de détecter toute identité non gérée, mal configurée ou exposée. Les résultats de ces analyses vous sont présentés dans un rapport facile à assimiler. Celui-ci vous montre toutes les voies d'attaque disponibles et vous fournit une liste des identités que vous devez corriger en priorité.

Proofpoint en action

Une entreprise de financement automobile renforce ses fonctionnalités de sécurité pour mieux protéger ses identités.

Cette entreprise mondiale de financement automobile avait créé une infrastructure informatique étendue et complexe sur une période de 30 ans. Bien qu'elle ait mis en place un système PAM, seuls quelques comptes sur ses applications héritées étaient gérés par celui-ci. Certains comptes administrateur et de service en étaient même exclus. L'entreprise ne pouvait donc pas gérer complètement ses identités et ses identifiants de connexion à privilèges, ni visualiser tous les risques liés à ses identités.

Lors d'un examen de routine de l'approche de l'entreprise en matière d'évaluation automatisée des risques, l'équipe de sécurité informatique a constaté qu'elle ne disposait d'aucun moyen de gérer les risques liés à ses identités. Elle a donc choisi Proofpoint Spotlight pour corriger cette faille de sécurité. Peu de temps après, Proofpoint a été intégré aux endpoints (clients et serveurs) et à l'infrastructure Active Directory (AD) de l'entreprise. Il a alors commencé à analyser tous ses endpoints, son système PAM et d'autres référentiels d'identités à la recherche de vulnérabilités.

L'équipe de sécurité informatique de l'entreprise a organisé une réunion avec l'équipe chargée de la correction des vulnérabilités informatiques afin de passer en revue ses conclusions. Les deux équipes ont décidé qu'il était préférable qu'elles travaillent ensemble pour mettre en place les changements nécessaires pour réduire les risques liés aux identités. Elles ont également suivi l'impact de ces changements au fil du temps.

Après plus d'un an d'utilisation de Proofpoint Spotlight, les équipes ont obtenu des résultats impressionnants. Même si plusieurs nouveaux problèmes critiques apparaissaient encore chaque semaine, elles disposaient désormais de nouveaux processus pour les résoudre rapidement.

« [Proofpoint Spotlight] nous a offert de nouvelles perspectives. Auparavant, nous savions que nous devions nous attarder davantage sur les risques liés aux identités, mais nous n'avions aucun moyen de le faire. »

– Assistant Vice President, IT Vulnerabilities, Entreprise de financement automobile

Principaux points à retenir

Il suffit d'une seule vulnérabilité liée à une identité pour mettre à mal tout votre environnement. Vous avez besoin d'outils capables de mettre en lumière les vulnérabilités liées à vos identités afin que vous puissiez identifier les risques et les réduire au fil du temps. Vous pourrez ainsi verrouiller des milliers de portes menant à des identités avant que des cyberpirates n'aient l'occasion d'essayer de les ouvrir.

AD et les systèmes d'identité sont complexes et évoluent constamment, ce qui entraîne l'introduction fréquente des risques liés aux identités.

Lorsqu'une personne est à l'origine de la compromission d'une identité, ce n'est généralement pas par malveillance, mais plutôt parce qu'elle a commis une erreur ou qu'elle était pressée.

CAS D'UTILISATION 2 :

Réussir les exercices de simulation d'attaques

Même en cas d'échec des défenses, les véritables gagnants des exercices de simulation d'attaques sont les entreprises qui les utilisent pour renforcer leur niveau de sécurité. Néanmoins, lorsqu'un exercice expose des identités non gérées ou mal configurées au sein de votre environnement, ce n'est jamais une bonne nouvelle. Mais rassurez-vous : presque tout le monde passe par là. En effet, 95 % des outils de simulation d'attaques identifient des identifiants de connexion d'administrateurs de domaine exposés lors des exercices[2].

2. Étude d'Illusive

Résumé

L'équipe SOC d'une banque de détail utilise Proofpoint pour empêcher un outil de simulation d'attaques de se connecter à ses comptes critiques et de compromettre ses serveurs.

Profil client

Secteur d'activité : Finance

Collaborateurs : 1 000

Lieu : EMEA

Solution

Produit : Proofpoint Identity Protection

Composant : Proofpoint Shadow

Comment Proofpoint peut vous aider

Proofpoint Identity Protection peut vous aider à détecter les attaques au milieu de la chaîne d'attaque et à empêcher un outil de simulation d'attaques d'atteindre son but sans être détecté.

- **Proofpoint Shadow** crée un réseau complexe de fausses données et voies d'accès à des ressources en apparence sensibles, puis les diffuse dans toute l'entreprise. Même les outils de simulation d'attaques les plus avancés ne savent pas distinguer le vrai du faux. La seule façon pour eux de faire la différence est d'essayer d'utiliser ce qu'ils ont découvert, ce qui avertira les équipes de sécurité de leur présence. Avec ce réseau de leurres, il est presque impossible pour eux de se déplacer vers des ressources informatiques stratégiques sans être détectés.
- **Proofpoint Spotlight** peut vous aider à identifier toutes les identités non gérées, mal configurées et exposées au sein de votre environnement. Vous pourrez ainsi les corriger avant que les outils de simulation d'attaques — et les cybercriminels — ne puissent les exploiter.

Proofpoint en action

Une grande banque de détail bloque deux simulations d'attaques.

Une grande banque de détail et d'investissement disposait de multiples couches de contrôles de sécurité ainsi que de plusieurs outils destinés à bloquer les malwares sur les endpoints. Mais face à la multiplication des menaces persistantes avancées (APT), elle souhaitait ajouter de nouvelles fonctionnalités de détection à son arsenal. Elle a donc installé Proofpoint Shadow. Peu de temps après, la banque a engagé une entreprise réputée spécialisée dans les tests d'intrusion pour attaquer son réseau. Elle s'est toutefois abstenue de prévenir l'entreprise qu'elle utiliserait Proofpoint pour déjouer ses assauts.

Avant le début du test d'intrusion, Proofpoint Shadow a introduit de fausses données destinées à attirer les cybercriminels sur chaque endpoint du réseau de 5 000 nœuds de la banque. Toutes les données ont été personnalisées pour donner l'impression d'appartenir à un environnement bancaire, y compris de faux identifiants de connexion.

Le premier jour du test, Proofpoint Shadow a détecté des tentatives d'activité malveillante provenant d'un faux utilisateur (« utilisateur A ») sur l'un des serveurs Citrix de la banque. Il a donc recueilli des informations sur les tenants et aboutissants (« qui, quoi, quand et où ») de l'attaque et a alerté les équipes SOC et de réponse aux incidents.

Lors de leurs investigations, les équipes ont découvert que les spécialistes en tests d'intrusion avaient installé des outils malveillants sur le réseau de la banque et tentaient d'utiliser d'autres faux comptes, collectés après la compromission initiale, pour faire progresser leur attaque. Les spécialistes en tests d'intrusion n'avaient aucune idée qu'ils avaient déjà été repérés par les équipes de sécurité.

Ensuite, le 22e jour, Proofpoint Shadow a envoyé une autre alerte concernant une nouvelle activité malveillante de l'utilisateur A, mais sur un serveur différent. Lorsque l'équipe SOC a procédé à une seconde analyse d'investigation numérique, elle a découvert des tentatives agressives de connexion à des comptes critiques via ce serveur. Le cybercriminel avait involontairement déclenché l'alerte en utilisant deux ensembles différents de faux identifiants de connexion.

Principaux points à retenir

Si votre équipe SOC peut réussir des exercices de simulation d'attaques, il y a plus de chances qu'elle soit capable de bloquer de véritables cybercriminels s'ils viennent à cibler votre environnement.

La détection précoce des comportements suspects permet aux équipes SOC et de sécurité des informations de neutraliser les cyberpirates avant qu'ils ne se déplacent latéralement et qu'ils n'atteignent les ressources informatiques stratégiques d'une entreprise. Ces détections incluent également des données précieuses, de sorte que les équipes peuvent soumettre les attaques à une analyse d'investigation numérique, ce qui facilite la réponse aux incidents et la réduction des risques.

La détection d'une tentative de craquage de mot de passe sur un faux compte garantit une alerte extrêmement fiable — un vrai positif indiquant une activité malveillante sur le réseau avec un taux de confiance de 100 %.

CAS D'UTILISATION 3 :

Sécuriser les identités hybrides dans AD et Entra ID

Active Directory (AD) est une pierre angulaire de l'infrastructure informatique des entreprises modernes. D'après certaines estimations, 90 % des entreprises utilisent AD comme principale méthode d'authentification et d'autorisation des utilisateurs. À l'ère de la migration vers le cloud, Microsoft Entra ID (anciennement Azure AD) devient lui aussi omniprésent.

Cependant, bien que populaires, ces outils sont également réputés pour être difficiles à gérer et à maintenir, en particulier parce qu'ils touchent presque tous les emplacements, utilisateurs et terminaux sur le réseau. Tout comme pour les outils IAM, les efforts consentis ne sont jamais pleinement récompensés, car les autorisations, les utilisateurs et les organisations évoluent constamment. Qui plus est, toutes les identités ne sont pas couvertes. Prenons l'exemple des identifiants de connexion mis en cache sur des endpoints. AD et Entra ID ne les gèrent pas — et les systèmes IAM non plus. Ils représentent donc un risque non négligeable.

Résumé

Une société de portefeuille bancaire utilise Proofpoint pour évaluer le niveau de sécurité d'une nouvelle acquisition et découvre 3 000 administrateurs de domaine sur ses postes de travail.

Profil client

Secteur d'activité : Finance

Collaborateurs : 25 000

Lieu : États-Unis

Solution

Produit : Proofpoint Identity Protection

Composant : Proofpoint Spotlight

Comment Proofpoint peut vous aider

Proofpoint Spotlight analyse AD, Entra ID et de nombreux autres référentiels d'identités et détecte les comptes qui disposent de privilèges qu'ils ne devraient pas avoir. En outre, il identifie les identités non gérées sur les endpoints, ainsi que les identités à privilèges qui ne sont pas gérées par la solution PAM ou d'autres systèmes IAM. Vous pouvez ainsi les corriger avant qu'elles ne tombent entre de mauvaises mains.

Proofpoint Spotlight offre également une vue ascendante et descendante sur les risques liés à vos identités non gérées, mal configurées et exposées. Les équipes de sécurité obtiennent ainsi une visibilité sur les voies d'attaque que les cybercriminels pourraient utiliser pour déployer des ransomwares et voler des données.

Proofpoint en action

Une société de portefeuille évalue les risques liés aux identités d'une nouvelle acquisition pour conclure la fusion-acquisition en toute sécurité.

Avec près de 200 milliards de dollars d'actifs et 1 000 succursales, cette société régionale de portefeuille bancaire acquiert une nouvelle banque tous les trois ans. À chaque fusion-acquisition, son équipe informatique combine des systèmes, des logiciels, des données et des processus. Mais avant cela, la société de portefeuille doit évaluer la sécurité de la banque qu'elle achète. Dans cet exemple, l'équipe disposait de moins de quatre mois pour effectuer son évaluation.

Le niveau de sécurité d'une banque dépend entièrement de la sécurité de ses identités. L'équipe informatique de la banque savait que si elle pouvait identifier les vulnérabilités liées aux identités de la nouvelle acquisition, elle obtiendrait une idée précise de son niveau de sécurité.

Au cours des six derniers mois, l'équipe avait utilisé Proofpoint Identity Protection pour analyser ses propres postes de travail et référentiels d'identités. Ses informations précieuses lui étaient donc familières. C'est pourquoi elle a décidé d'utiliser Proofpoint Spotlight pour procéder à l'évaluation initiale de la banque acquise.

« Je suis ravi que nous ayons utilisé [Proofpoint Spotlight], tout le monde a perçu ses avantages. Nous procéderons de la même manière lors de notre prochaine fusion-acquisition. »

– Directeur de l'ingénierie de cybersécurité

Après avoir analysé l'environnement informatique de la nouvelle acquisition, Proofpoint a généré un tableau de bord des risques, qui détaillait plusieurs domaines de risque liés aux identités. L'un d'entre eux s'est rapidement détaché des autres : les postes de travail comportaient 3 000 comptes d'administrateurs de domaine. Il suffirait que l'un d'eux soit compromis par un cybercriminel pour que l'équipe perde le contrôle de l'ensemble de l'environnement.

Après avoir pris connaissance des pratiques de sécurité de la nouvelle banque, les dirigeants ont décidé que, compte tenu des risques, il était préférable de garder les deux environnements informatiques séparés, du moins dans un premier temps. Sans Proofpoint, il aurait été beaucoup plus difficile de justifier le renforcement de la protection que l'équipe informatique jugeait nécessaire.

Principaux points à retenir

Bien souvent, les risques liés aux identités résultent de processus métier et informatiques ordinaires qui sont en place depuis de nombreuses années. Ils sont donc difficiles à détecter et faciles à négliger, en particulier dans les environnements récemment acquis suite à une fusion-acquisition.

Il est essentiel d'analyser constamment AD, Entra ID, les endpoints et autres référentiels à la recherche de vulnérabilités liées aux identités. Un cybercriminel n'a besoin de compromettre qu'un seul poste de travail avec un seul utilisateur pour prendre le contrôle de tout un environnement.

Conclusion

La plupart des entreprises recherchent régulièrement les logiciels et applications vulnérables, mais elles oublient généralement les identités vulnérables. Pourtant, les identités ont une valeur inestimable. À bien des égards, il s'agit des ressources les plus précieuses des entreprises, car elles concernent tous les autres actifs numériques.

Leur protection revêt donc une importance capitale. Les cybercriminels ont aujourd'hui accès à un large éventail d'outils qui leur permettent d'exploiter des identifiants de connexion de manière rapide, facile et efficace. Pire encore, il est difficile pour les entreprises de détecter leur utilisation.

Pour briser la chaîne d'attaque, vous devez protéger vos identités comme vous protégez toutes les autres ressources stratégiques. Cela commence par la prise de mesures proactives. Vous devez corriger vos identités vulnérables avant que des cyberpirates ne les découvrent et utiliser des leurres pour intercepter les cybercriminels avant qu'ils ne fassent des dégâts.

Pour découvrir comment Proofpoint peut vous aider à protéger vos identités, consultez la page : https://www.proofpoint.com/us/products/identity-protection.

EN SAVOIR PLUS

Pour plus d'informations, visitez notre site à l'adresse : **proofpoint.com/fr**.

À PROPOS DE PROOFPOINT

Proofpoint, Inc. est une entreprise leader dans le domaine de la cybersécurité et de la conformité qui protège les ressources les plus importantes et les plus à risques des entreprises : leurs collaborateurs. Grâce à une suite intégrée de solutions cloud, Proofpoint aide les entreprises du monde entier à stopper les menaces ciblées, à protéger leurs données et à rendre leurs utilisateurs plus résistants face aux cyberattaques. Les entreprises de toutes tailles, y compris 85 % des entreprises de l'index Fortune 100, font confiance aux solutions de sécurité et de conformité de Proofpoint centrées sur les personnes, pour diminuer leurs risques les plus critiques via les emails, le cloud, les réseaux sociaux et le Web. Pour plus d'informations, rendez-vous sur **www.proofpoint.com/fr**.